(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－49867
（Ｐ2000－49867Ａ）
(43)公開日　平成12年２月18日(2000.2.18)

(51)Int.Cl.⁷		識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｌ	12/56		Ｈ０４Ｌ	11/20	１０２Ａ
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｚ
Ｈ０４Ｌ	12/46		Ｈ０４Ｌ	11/00	３１０Ｃ
	12/28				

審査請求　未請求　請求項の数18　ＯＬ　（全 16 頁）

(21)出願番号　特願平11－151071

(22)出願日　平成11年５月31日(1999.5.31)

(31)優先権主張番号　０９／０８７８２３

(32)優先日　平成10年５月29日(1998.5.29)

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591064003
サン・マイクロシステムズ・インコーポレーテッド
ＳＵＮ　ＭＩＣＲＯＳＹＳＴＥＭＳ，ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国　94303　カリフォルニア州・パロ　アルト・サン　アントニオ　ロード・901

(74)代理人　100064621
弁理士　山川　政樹

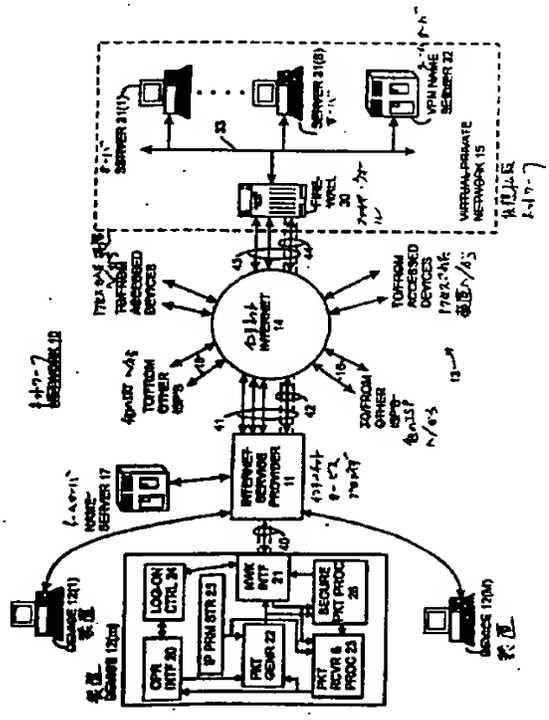
最終頁に続く

(54)【発明の名称】　インターネットなどの公衆ネットワークに接続された装置とネットワークに接続された装置の間の通信を容易にするシステムおよび方法

(57)【要約】

【課題】　仮想私設ネットワーク内の内部装置と外部装置との通信時のインターネットの人間可読アドレスなどの二次アドレスからネットワーク・アドレスへの変換を容易にするシステム。

【解決手段】　仮想私設ネットワークはファイヤウォールと、少なくとも１つの内部装置と、ネームサーバとを有する。それぞれネットワーク・アドレスを有する。内部装置は二次アドレスも有し、ネームサーバは二次アドレスとネットワーク・アドレスとの間を関連づける。ファイアウォールは、外部装置との接続の確立を求める外部装置からの要求に応答し、外部装置にネームサーバのネットワーク・アドレスを供給する。外部装置は、内部装置の二次アドレスを含む、内部装置へのアクセスを要求する操作者などからの要求に応答してネットワーク・アドレス要求メッセージを生成し、ファイアウォールとの接続を介して送信し、二次アドレスに関連づけられたネットワーク・アドレスの変換を要求する。



【特許請求の範囲】

【請求項１】　ディジタル・ネットワークを介して通信する仮想私設ネットワークと外部装置とを含むシステムであって、

前記仮想私設ネットワークは、それぞれネットワーク・アドレスを有するファイアウォールと、少なくとも１つの内部装置と、ネームサーバとを有し、前記内部装置は二次アドレスも有し、前記ネームサーバは前記二次アドレスと前記ネットワーク・アドレスとの間を関連づけるように構成され、

前記ファイアウォールは、そのファイアウォールと外部装置との間の接続の確立を求める外部装置からの要求に応答し、その外部装置に前記ネームサーバのネットワーク・アドレスを供給するように構成され、

前記外部装置は、前記内部装置の二次アドレスを含む前記内部装置へのアクセスを要求する要求に応答し、前記ファイアウォールへの接続を介して送信するために、前記二次アドレスに関連づけられた前記ネットワーク・アドレスの変換を要求するネットワーク・アドレス要求メッセージを生成し、前記ファイアウォールは前記ネームサーバに前記アドレス変換要求を供給するように構成され、前記ネームサーバは前記二次アドレスに関連づけられた前記ネットワーク・アドレスを供給するように構成され、前記ファイアウォールはさらに前記外部装置への接続を介して送信するためにネットワーク・アドレス応答メッセージで前記ネットワーク・アドレスを供給するように構成されたシステム。

【請求項２】　前記外部装置が、前記内部装置への送信のために少なくとも１つのメッセージを生成する際に前記ネットワーク・アドレス応答メッセージで供給された前記ネットワーク・アドレスを使用するように構成された請求項１に記載のシステム。

【請求項３】　前記外部装置がネットワーク・サービス・プロバイダを介して前記ネットワークに接続された請求項１に記載のシステム。

【請求項４】　前記外部装置が、前記ネットワーク・サービス・プロバイダとの通信セッションを確立するように構成され、前記ネットワーク・サービス・プロバイダが前記外部装置に他のネームサーバの識別情報を提供し、前記他のネームサーバは少なくとも１つの装置のために二次アドレスとネットワーク・アドレスとの間を関連づけるように構成された請求項３に記載のシステム。

【請求項５】　前記外部装置が、前記外部装置に知らされているネームサーバのリストを維持するように構成され、前記外部装置が他の装置へのアクセスを要求する要求に応答して、前記外部装置がネットワーク・アドレスを受け取るまで前記リスト内のネームサーバのうちの連続したネームサーバに問い合わせるように構成され、前記要求が前記他の装置の二次アドレスを含み、各問い合わせで前記外部装置がネットワークを介して送信するために、前記リスト内の前記ネームサーバのうちの１つのネームサーバによる応答を求める前記ネットワーク・アドレス要求メッセージを生成し、前記１つのネームサーバからネットワーク・アドレス応答メッセージを受け取るように構成された請求項１に記載のシステム。

【請求項６】　前記外部装置と前記ファイアウォールとの間の接続が、前記外部装置と前記ファイアウォールとの間で伝送されるメッセージの少なくとも一部が暗号化されるセキュア・トンネルである請求項１に記載のシステム。

【請求項７】　仮想私設ネットワークが、それぞれネットワーク・アドレスを有するファイアウォールと少なくとも１つの内部装置とネームサーバとを有し、前記内部装置は二次アドレスも有し、前記ネームサーバが前記二次アドレスと前記ネットワーク・アドレスとの間を関連づけるように構成された、ディジタル・ネットワークによって相互接続された仮想私設ネットワークと外部装置とを含むシステムを動作させる方法であって、

Ａ．前記ファイアウォールと外部装置との間の接続の確立を求める外部装置からの要求に応答してファイアウォールをイネーブルし、その外部装置に前記ネームサーバのネットワーク・アドレスを供給するステップと、

Ｂ．（ｉ）前記外部装置が、前記内部装置の二次アドレスを含む前記内部装置へのアクセスを要求する要求に応答して、前記ファイアウォールへの接続を介して送信するために、前記二次アドレスに関連づけられた前記ネットワーク・アドレスの変換を要求するネットワーク・アドレス要求メッセージを生成するステップと、

（ii）前記ファイアウォールが、前記ネームサーバに前記アドレス変換要求を供給するステップと、

（iii）前記ネームサーバが、前記二次アドレスに関連づけられた前記ネットワーク・アドレスを供給するステップと、

（iv）前記ファイアウォールが、前記外部装置への接続を介して送信するためにネットワーク・アドレス応答メッセージで前記ネットワーク・アドレスを供給するステップとを含む方法。

【請求項８】　前記外部装置がさらに、前記内部装置への送信のために少なくとも１つのメッセージを生成する際に前記ネットワーク・アドレス応答メッセージで供給された前記ネットワーク・アドレスを使用することができるようにされる請求項７に記載のシステム。

【請求項９】　前記外部装置がネットワーク・サービス・プロバイダを介して前記ネットワークに接続できるようにされる請求項７に記載のシステム。

【請求項１０】　前記外部装置が、前記ネットワーク・サービス・プロバイダとの通信セッションを確立することができるようにされ、前記ネットワーク・サービス・プロバイダが前記外部装置に他のネームサーバの識別情報を提供することができるようにされ、前記他のネーム

サーバは少なくとも１つの装置のために二次アドレスとネットワーク・アドレスとの間の関連づけを提供することができるようにされる請求項９に記載のシステム。

【請求項１１】　前記外部装置が、前記外部装置に知らされているネームサーバのリストを維持することができるようにされ、前記外部装置が他の装置へのアクセスを要求する要求に応答して、前記外部装置がネットワーク・アドレスを受け取るまで前記リスト内のネームサーバのうちの連続したネームサーバに問い合わせることができるようにされ、前記要求が前記他の装置の二次アドレスを含み、各問い合わせで前記外部装置がネットワークを介して送信するために、前記リスト内の前記ネームサーバのうちの１つのネームサーバによる応答を求める前記ネットワーク・アドレス要求メッセージを生成し、前記１つのネームサーバからネットワーク・アドレス応答メッセージを受け取ることができるようにされる請求項７に記載のシステム。

【請求項１２】　前記外部装置と前記ファイアウォールとの間の接続が、前記外部装置と前記ファイアウォールとの間で伝送されるメッセージの少なくとも一部が暗号化されるセキュア・トンネルである請求項７に記載の方法。

【請求項１３】　仮想私設ネットワークが、それぞれネットワーク・アドレスを有するファイアウォールと、少なくとも１つの内部装置と、ネームサーバとを有し、前記内部装置は二次アドレスも有し、前記ネームサーバは前記二次アドレスと前記ネットワーク・アドレスとの間を関連づけるように構成された、ディジタル・ネットワークによって相互接続された仮想私設ネットワークと外部装置との接続に使用するコンピュータ・プログラム製品であって、

Ａ．前記ファイアウォールが、そのファイアウォールと外部装置との間の接続の確立を求める外部装置からの要求に応答し、前記外部装置に前記ネームサーバのネットワーク・アドレスを供給することができるようにするように構成されたネームサーバ識別コード・モジュールと、

Ｂ．前記外部装置が、前記内部装置の二次アドレスを含む前記内部装置へのアクセスを要求する要求に応答し、前記ファイアウォールへの接続を介して送信するために、前記二次アドレスに関連づけられた前記ネットワーク・アドレスの変換を要求するネットワーク・アドレス要求メッセージを生成することができるようにするネットワーク・アドレス要求メッセージ生成コード・モジュールと、

Ｃ．前記ファイアウォールが、前記ネームサーバに前記アドレス変換要求を供給することができるようにするアドレス変換要求転送モジュールと、

Ｄ．前記ネームサーバが前記二次アドレスに関連づけられた前記ネットワーク・アドレスを供給することができるようにするネームサーバ制御モジュールと、

Ｅ．前記ファイアウォールが、前記外部装置への接続を介して送信するためにネットワーク・アドレス応答メッセージで前記ネットワーク・アドレスを供給することができるようにするネットワーク・アドレス応答メッセージ転送モジュールとがコード化された機械可読媒体を含むコンピュータ・プログラム製品。

【請求項１４】　前記外部装置が前記内部装置への送信のために少なくとも１つのメッセージを生成する際に前記ネットワーク・アドレス応答メッセージで供給された前記ネットワーク・アドレスを使用することができるようにするように構成されたネットワーク・アドレス使用モジュールをさらに含む請求項１３に記載のコンピュータ・プログラム製品。

【請求項１５】　前記外部装置がネットワーク・サービス・プロバイダを介して前記ネットワークに接続できるようにするネットワーク・サービス・プロバイダ制御モジュールをさらに含む請求項１３に記載のコンピュータ・プログラム製品。

【請求項１６】　前記ネットワーク・サービス・プロバイダ制御モジュールが、前記外部装置を前記ネットワーク・サービス・プロバイダとの通信セッションのためにイネーブルにし、前記ネットワーク・サービス・プロバイダから他のネームサーバの識別情報を受け取ることができるようにする、通信セッション確立モジュールを含む請求項１５に記載のコンピュータ・プログラム製品。

【請求項１７】　前記外部装置が前記外部装置に知らされているネームサーバのリストを維持することができ、前記外部装置が他の装置へのアクセスを要求する要求に応答して、前記外部装置がネットワーク・アドレスを受け取るまで前記リスト内のネームサーバのうちの連続したネームサーバに問い合わせることができるようにするネームサーバ問合わせ制御モジュールであって、前記要求が前記他の装置の二次アドレスを含み、各問い合わせで前記外部装置がネットワークを介して送信するために、前記リスト内の前記ネームサーバのうちの１つのネームサーバによる応答を求める前記ネットワーク・アドレス要求メッセージを生成し、前記１つのネームサーバからネットワーク・アドレス応答メッセージを受け取ることができるようにするネームサーバ問合わせ制御モジュールをさらに含む請求項１３に記載のコンピュータ・プログラム製品。

【請求項１８】　前記外部装置と前記ファイアウォールとの間の接続が、前記外部装置と前記ファイアウォールとの間で伝送されるメッセージの少なくとも一部が暗号化されるセキュア・トンネルである請求項１４に記載のコンピュータ・プログラム製品。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、一般にはディジタ

ル通信システムおよび方法に関し、より詳細には、インターネットなどの公衆ネットワークに接続された装置と私設ネットワークに接続された装置との間の通信を容易にするシステムおよび方法に関する。

【０００２】

【従来の技術】ディジタル・コンピュータ・システムおよびその他のディジタル装置間でのデータおよびプログラムを含む情報の伝送を容易にするために、ディジタル・ネットワークが開発されている。多様な情報伝送方法を使用して情報を伝送する、いわゆる「ワイド・エリア・ネットワーク」（ＷＡＮ）や「ローカル・エリア・ネットワーク」（ＬＡＮ）を含む様々なタイプのネットワークが開発され、実施されている。一般に、ＬＡＮは、特定の事務所、会社、またはより小規模なタイプの組織内で特定の情報を伝送するために、個々の事務所施設内などの比較的狭い地理的区域にわたって実施される。他方、ＷＡＮは一般に、比較的広い地理的区域にわたって実施され、ＬＡＮ間およびＬＡＮに接続されていない装置間で情報を伝送するために使用することができる。ＷＡＮは、複数の会社のために情報を伝達することができるインターネットなどの公衆ネットワークも含む。

【０００３】ネットワーク、特に、インターネットなどの大規模な公衆ＷＡＮを介した通信に関してはいくつかの問題が生じている。一般に、情報はメッセージ・パケットの形でネットワークを介して伝送され、パケットは送信元装置としての１つの装置から宛先装置としての他の装置に、ネットワーク内の１つまたは複数のルータまたはスイッチング・ノード（一般にはスイッチング・ノード）を介して伝送される。各メッセージ・パケットは宛先アドレスを含み、スイッチング・ノードはそれを使用してそれぞれのメッセージ・パケットを適切な宛先装置に経路指定する。インターネットを介したアドレスは、「ｎ」ビット整数の形式（「ｎ」は３２または１２８）であり、人が覚えたり、メッセージ・パケットを送信できるようにしたい場合にそれを入力したりするのが難しい。ユーザが特定の整数インターネットアドレスを覚えたり入力したりする必要を軽減するために、インターネットは、それぞれの装置の操作者によってより容易に使用される第２のアドレス指定機構を備える。このアドレス指定機構では、インターネットに接続されたＬＡＮ、インターネット・サービス・プロバイダ（「ＩＳＰ」）などのインターネット・ドメインが、比較的人間が読みやすい名前で識別される。この人間可読名の使用に対応するために、ＤＮＳサーバとも呼ばれるネームサーバが設けられ、人間可読名を適切なインターネット・アドレスに変換する。１台の装置の操作者が、メッセージ・パケットを他の装置に送信しようとして他方の装置の人間可読名を入力すると、その装置は最初にネームサーバに接触する。一般に、ネームサーバはＩＳＰ自体の一部とするか、またはＩＳＰを介してインターネットでアクセス可能な特定の装置とすることができる。いずれの場合も、ＩＳＰは、装置がＩＳＰにログインすると、使用するネームサーバをその装置に知らせる。装置によって接触された後で、ネームサーバがその人間可読ドメイン名の整数インターネット・アドレスを持っているかまたは入手可能な場合、ネームサーバはその人間可読ドメイン名に対応する整数インターネット・アドレスを操作者の装置に提供する。その後、装置はネームサーバによって返された整数インターネット・アドレスをメッセージ・パケットに入れ、そのメッセージ・パケットを従来の方式でインターネットを介して送信するためにＩＳＰに供給する。インターネット・スイッチング・ノードは、整数インターネット・アドレスを使用してメッセージ・パケットを意図された宛先装置に経路指定する。

【０００４】特にインターネットなどの公衆ＷＡＮを介した情報伝送に関しては他の問題も生じる。１つの問題は、ＷＡＮを介して転送される情報であって、送信元装置と宛先装置が機密にしておきたい情報が、その情報を傍受する可能性のある盗聴者に対して機密に維持されるように保証することである。機密性を維持するには、様々な形態の暗号化が開発され、送信元装置による伝送の前に情報を暗号化し、宛先装置によって受け取られた後で情報を復号するために使用されている。たとえば、特定の送信元装置と特定の宛先装置との間で伝送されるすべての情報を機密に維持することが望ましい場合、それらの装置は両者の間に「セキュア・トンネル」を設定することができる。このセキュア・トンネルは本質的に、伝送の前に送信元装置によって宛先装置に伝送されるすべての情報（ただし、アドレス情報など、送信元装置と宛先装置の間のネットワークを介したネットワーク・パケットの流れを制御する特定のプロトコル情報は除く）が暗号化されるように保証し、暗号化された情報が宛先装置によって使用される前に復号されるように保証する。送信元装置と宛先装置はそれ自体がそれぞれ暗号化と復号を実行するか、または、メッセージ・パケットがインターネットを介して伝送される前に他の装置が暗号化と復号を行うことができる。

【０００５】特に、ＬＡＮ、ＷＡＮ、またはそれらの任意の組合せである私設ネットワークがインターネットなどの公衆ＷＡＮに接続されている会社、政府機関、および民間組織に対して生じる他の問題は、それらの私設ネットワークが、それらの会社がアクセスさせたくない他者から保護されるように保証すること、またはそれぞれの組織がアクセスを制限したい他者によるアクセスを規制または管理することである。これに対応するために、組織は一般に、その私設ネットワークを「ファイアウォール」と呼ばれることがある限定された数のゲートウェイを介してＷＡＮに接続し、内部ネットワークと公衆ネットワークとの間のすべてのネットワーク・トラフィックがこのファイアウォールを通るようにする。一般に、

ファイアウォールの「背後」にある私設ネットワーク内のドメインおよび装置のネットワーク・アドレスは、私設ネットワーク内に設けられたネームサーバにはわかっているが、私設ネットワーク外部のネームサーバやその他の装置には入手できず、私設ネットワーク外部の装置と私設ネットワーク内部の装置との間の通信を困難にする。

【０００６】

【発明が解決しようとする課題】本発明は、私設ネットワークに接続されたネームサーバまたは同様のものによるインターネットの人間可読アドレスなどの二次アドレスからネットワーク・アドレスへの変換を容易にすることによって、インターネットなどの公衆ネットワークに接続された装置と私設ネットワークに接続された装置との間の通信を容易にする、新規な改良されたシステムおよび方法を提供する。

【０００７】

【課題を解決するための手段】要約すると、本発明は、仮想私設ネットワークと、ディジタル・ネットワークによって相互接続された外部装置とを含むシステムを提供する。仮想私設ネットワークは、ファイアウォールと、少なくとも１つの内部装置と、ネームサーバとを有し、それぞれがネットワーク・アドレスを有する。内部装置は、二次アドレスも有し、ネームサーバは二次アドレスとネットワーク・アドレスとの間の関連づけを行うように構成されている。ファイアウォールは、外部装置との間の接続の確立を求める外部装置からの要求に応答し、外部装置にネームサーバのネットワーク・アドレスを提供する。外部装置は、内部装置へのアクセスを要求する内部装置の二次アドレスを含む操作者などからの要求に応答し、ネットワーク・アドレス要求メッセージを生成してファイアウォールまでの接続を介して送信し、二次アドレスに関連づけられたネットワーク・アドレスの変換を要求する。ファイアウォールはそのアドレス変換要求をネームサーバに供給し、ネームサーバは二次アドレスに関連づけられたネットワーク・アドレスをファイアウォールに供給する。ファイアウォールは、外部装置までの接続を介して送信するためにネットワーク・アドレス応答メッセージでネットワーク・アドレスを供給する。その後、外部装置は、このようにして供給されたネットワーク・アドレスを、内部装置宛に意図されたファイアウォールとのその後の通信で使用することができる。

【０００８】

【発明の実施の形態】本発明は、特許請求の範囲で具体的に示されている。本発明の上記およびその他の利点は、添付図面と共に以下の説明を参照すればよりよく理解できよう。

【０００９】図１は、本発明により構成されたネットワーク１０を示す機能ブロック図である。図１に図示するネットワーク１０は、インターネット・サービス・プロバイダ（「ＩＳＰ」）１１に接続された１つまたは複数の装置１２（１）～１２（Ｍ）（一般的に参照番号１２（ｍ）で識別する）および参照番号１３で一般的に識別されたその他の装置間の、インターネット１４を介したメッセージ・パケットの伝送を容易にし、それによって装置１２（ｍ）と１３と間でのメッセージ・パケットでの情報の伝送を容易にするインターネット・サービス・プロバイダ（「ＩＳＰ」）１１を含む。ＩＳＰ１１は、参照番号４１で一般的に識別された１つまたは複数の論理接続またはゲートウェイまたは同様のもの（本明細書では総称して「接続」と呼ぶ）を介してインターネット１４に接続する。ＩＳＰ１１は、公衆ＩＳＰとすることができ、その場合、一般社会の構成員である操作者が制御することができる装置１２（ｍ）に接続され、それらの操作者がインターネットへアクセスできるようにする。あるいは、ＩＳＰ１１は私設ＩＳＰとすることができ、その場合、それに接続された装置１２（ｍ）は一般に、たとえば特定の会社または政府機関の従業員、民間組織のメンバーなどによって操作され、それらの従業員またはメンバーがインターネットへアクセスできるようにする。

【００１０】従来、インターネットは、ＩＳＰ１１および装置１３を相互接続してそれらの間のメッセージ・パケットの伝送を容易にするスイッチング・ノード（別途図示せず）の網を含む。インターネット１４を介して伝送されるメッセージ・パケットは、いわゆるインターネット・プロトコル「ＩＰ」によって定義されたものに準拠し、ヘッダ部分とデータ部分とを含み、誤り検出または訂正あるいはその両方の部分を含むことができる。ヘッダ部分には、たとえば、そのメッセージ・パケットを受け取るべき装置を宛先装置として識別する宛先アドレスと、メッセージ・パケットを生成した装置を識別する送信元アドレスを含めて、インターネット１４を介してメッセージ・パケットを伝送するために使用される情報が含まれる。各メッセージ・パケットについて、宛先アドレスと送信元アドレスはいずれも、それぞれの宛先装置と送信元装置を固有に識別する整数の形態をとる。宛先装置がインターネット、またはＩＳＰ１１、あるいはインターネット１４に接続されたその他の装置に接続されている場合、インターネット１４を構成するスイッチング・ノードは、少なくともそれぞれのメッセージ・パケットの宛先アドレスを使用して、それ（すなわちそれぞれのメッセージ・パケット）を宛先装置に経路指定する。インターネット、またはＩＳＰ１１あるいはインターネットに接続された装置は、そのメッセージ・パケットをその適切な宛先に転送する。各メッセージ・パケットのデータ部分には、メッセージ・パケットで伝送するデータと、メッセージ・パケットが送信元装置から宛先装置に正しく伝送されたことを検証する（誤り検出情報

の場合）ためと、メッセージ・パケットが正しく伝送されなかった場合に選択されたタイプの誤りを訂正する（誤り訂正情報の場合）ために使用することができる誤り検出および／または訂正情報を含む誤り検出および／または訂正部分とが含まれる。

【００１１】ＩＳＰ１１に接続される装置１２（ｍ）は、たとえば、パーソナル・コンピュータ、コンピュータ・ワークステーションなどインターネット１４を介して他の装置１３と通信するいくつかのタイプの装置のいずれをも含むことができる。各装置１２（ｍ）は、装置１２（ｍ）がポイントツーポイント・リンクを使用してＩＳＰ１１に接続される場合は周知のポイントツーポイント・プロトコル（「ＰＰＰ」）、装置１２（ｍ）がイーサネットなどの分岐ネットワークを介してＩＳＰ１１に接続される場合は従来の分岐ネットワーク・プロトコルなど、従来の任意のプロトコルを使用して、ＩＳＰ１１と通信し、インターネット１４で伝送するためにメッセージ・パケットをＩＳＰ１１に送信するか、またはインターネット１４を介してＩＳＰ１１が受け取ったメッセージ・パケットをＩＳＰ１１から受け取る。装置１２（ｍ）は一般に、たとえばシステム・ユニット、ビデオ表示装置、およびキーボードやマウスなどのオペレータ入力装置を含む、従来のプログラム記憶式コンピュータ・アーキテクチャにより構成される。システム・ユニットは、一般に、処理装置、メモリ、ディスクやテープ記憶要素などの大容量記憶装置、およびそれぞれの装置をＩＳＰ１１とインタフェースさせるネットワーク・インタフェース装置または電話インタフェース装置を含むその他の要素（別途に図示せず）を含む。処理装置は、オペレーティング・システムの制御下でアプリケーション・プログラムを含むプログラムを処理し、処理されたデータを生成する。ビデオ表示装置は、装置が処理されたデータと処理状況をユーザに対して表示することができるようにし、オペレータ入力装置は、ユーザがデータを入力し、処理を制御することができるようにする。

【００１２】装置１２（ｍ）のこれらの装置は、適切なプログラミングと共に、協調動作して、装置１２（ｍ）に、たとえばオペレータ・インタフェース２０、ネットワーク・インタフェース２１、メッセージ・パケット・ジェネレータ２２、メッセージ・パケット受信および処理機能要素２３、ＩＳＰログオン・コントロール２４、インターネット・パラメータ・ストア２５、および本発明に関係するセキュア・メッセージ・パケット処理機能要素２６を含む多くの機能要素を備えている。オペレータ・インタフェース２０は、装置１２（ｍ）での装置１２（ｍ）のオペレータ入力装置からの入力情報の受領と、装置１２（ｍ）のビデオ表示装置上での操作者に対する出力情報の表示を容易にする。ネットワーク・インタフェース２１は、適切なＰＰＰまたはネットワーク・プロトコルを使用して装置１２（ｍ）がＩＳＰ１１に接続し、ＩＳＰ１１にメッセージ・パケットを送信したり、ＩＳＰ１１からメッセージ・パケットを受け取ったりするのを容易にする。ネットワーク・インタフェース２１は、公衆電話ネットワークを介したＩＳＰ１１への接続を容易にし、公衆電話システムを介した装置１２（ｍ）のダイヤルアップ・ネットワーク化を可能にすることもできる。別法として、あるいはそれに加えて、ネットワーク・インタフェース２１は、たとえばイーサネットなどの従来のＬＡＮによるＩＳＰ１１を介した接続も容易にすることができる。ＩＳＰログオン・コントロール２４は、オペレーティング・インタフェース２０によって供給された入力に応答して、または装置１２（ｍ）によって処理されているプログラム（図示せず）からの要求に応答して、ネットワーク・インタフェース２１を介して通信し、装置１２（ｍ）とＩＳＰ１１との間の通信セッションの初期設定（「ログオン」）を容易にし、その通信セッション中に装置１２（ｍ）はメッセージ・パケットの形でインターネット１４を介して他の装置、およびＩＳＰ１１に接続された他の装置１２（ｍ’）（ｍ’≠ｍ）または他のＩＳＰに情報を送信することができる。ログオン動作中、ＩＳＰログオン・コントロール２４は、インターネット・プロトコル（「ＩＰ」）パラメータを受け取り、このパラメータは通信セッション中にメッセージ・パケット生成と共に使用される。

【００１３】通信セッション中、メッセージ・パケット・ジェネレータ２２は、オペレーティング・インタフェース２０を介して操作者によって供給された入力に応答して、または装置１２（ｍ）によって処理されているプログラム（図示せず）からの要求に応答して、ネットワーク・インタフェース２１を介した送信のためのメッセージ・パケットを生成する。ネットワーク・インタフェース２１は、ＩＳＰ１１からもメッセージ・パケットを受け取ってメッセージ・パケット受信および処理機能要素２３に送り、それらを処理させ、オペレータ・インタフェース２０または装置１２（ｍ）によって処理されているその他のプログラム（図示せず）に供給させる。受け取ったメッセージ・パケットに、操作者に対して表示するウェブ・ページなどの情報が含まれている場合、その情報をオペレータ・インタフェース２０に供給し、その装置の表示装置上に情報が表示されるようにすることができる。それに加えて、または別法として、情報は装置１２（ｍ）によって処理されている他のプログラム（図示せず）に処理のために供給することもできる。

【００１４】一般に、オペレーティング・インタフェース２０、メッセージ・パケット・ジェネレータ２２、メッセージ受信および処理機能要素２３、ＩＳＰログオン・コントロール２４、およびインターネット・パラメータ・ストア２５などの要素は、Ｍｏｓａｉｃ、Ｎｅｔｓｃａｐｅ Ｎａｖｉｇａｔｏｒ、ＭｉｃｒｏｓｏｆｔＩ

ｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒなどの従来のインターネット・ブラウザの要素を含むことができる。

【００１５】前述のように、本発明に関連して、装置１２（ｍ）はセキュア・メッセージ・パケット処理機能要素２６も含む。セキュア・メッセージ・パケット処理機能要素２６は、装置１２（ｍ）と他の装置１２（ｍ’）（ｍ’≠ｍ）または１３との間での後述の「セキュア・トンネル」の確立と使用を容易にする。一般に、セキュア・トンネルでは、装置１２（ｍ）と他の特定の装置１２（ｍ’）（ｍ’≠ｍ）または１３との間で伝送されるメッセージ・パケットの少なくともデータ部分内の情報が、たとえば送信元装置で、送信の前にデータ部分を暗号化することによって機密に維持される。このようなメッセージ・パケットの他の部分に入っている情報も機密に維持することができる。ただし、インターネットのスイッチング・ノードおよびＩＳＰがメッセージ・パケットを受け取るべき装置を識別することができるように、たとえば少なくとも宛先情報を含めて、装置間のそれぞれのメッセージ・パケットの伝送を助けるのに必要な情報は機密にされていない。

【００１６】ＩＳＰ１１に加えて、矢印１６でそれぞれ示すように他のいくつかのＩＳＰもインターネットに接続することができ、したがって、他の装置を有するそれらの他のＩＳＰに接続された装置と、ＩＳＰ１１に接続された装置１２（ｎ）を含む他の装置とのインターネットを介した通信も可能になる。

【００１７】装置１２（ｍ）がアクセスし、通信する装置１３も、パーソナル・コンピュータ、コンピュータ・ワークステーションなどを含めて任意の数のタイプの装置とすることができ、これには、ネットワークに直接または間接に接続可能なそのような装置や他の多くのタイプの装置を含む、ミニ・コンピュータ、メインフレーム・コンピュータ、大容量記憶システム、計算サーバ、ローカル・エリア・ネットワーク（「ＬＡＮ」）およびワイド・エリア・ネットワーク（「ＷＡＮ」）も含まれる。本発明に関しては、このような装置の少なくとも１つの装置は、仮想私設ネットワーク１５として識別される少なくとも１つの私設ネットワークを含み、これはＬＡＮまたはＷＡＮの形態をとることができる。仮想私設ネットワーク１５は、装置１２（ｍ’）（ｍ’≠ｍ）（ＩＳＰを介してインターネット１４に接続する）または１３（インターネット１４に直接接続する）のいずれの装置でも含むことができる。本明細書で説明する例示の実施形態では、仮想私設ネットワーク１５は装置１３を含むものとする。仮想私設ネットワーク１５自体は、本明細書でファイアウォール３０として示す複数の装置と、複数のサーバ３１（１）～３１（Ｓ）（一般的に参照番号３１（ｓ）で識別する）と、ネームサーバ３２とを含み、これらはすべて通信リンク３３によって相互接続されている。ファイアウォール３０およびサーバ３１（ｓ）は、本明細書に記載の様々なタイプの装置１２（ｍ）および１３のいずれともすることができ、したがって、たとえば、パーソナル・コンピュータ、コンピュータ・ワークステーションおよび同様のものを含むことができ、これには、ネットワークに直接または間接に接続可能なそのような装置や他の多くのタイプの装置を含むミニ・コンピュータ、メインフレーム・コンピュータ、大容量記憶システム、計算サーバ、ローカル・エリア・ネットワーク（「ＬＡＮ」）、およびワイド・エリア・ネットワーク（「ＷＡＮ」）も含まれる。

【００１８】前述のように、装置１２（ｍ）および装置１３を含む装置は、インターネットを介してメッセージ・パケットを伝送することによって通信する。装置１２（ｍ）および１３は、「ピアツーピア」方式、「クライアントーサーバ」方式、またはその両方の方式で情報を伝送することができる。一般に、「ピアツーピア」メッセージ・パケット伝送では、装置は１つまたは複数のメッセージ・パケットにした情報を他の装置に送信するに過ぎない。それに対して、「クライアントーサーバ」方式では、クライアントとして動作する装置が、サーバとして動作する他の装置にメッセージパケットを送信して、たとえば他方の装置によるサービスを開始することができる。たとえば他方の装置からの情報の検索、他方の装置が処理演算などを実行することができるようにすることなど、いくつかのタイプのこのようなサービスが、当業者にはわかるであろう。サーバがクライアントに情報を提供する場合、そのサーバは一般に記憶サーバと呼ぶことができる。それに対して、サーバがクライアントの要求により処理演算を実行する場合、そのサーバは一般に計算サーバと呼ぶことができる。クライアントの要求により他のタイプのサービスおよび操作を実行するサーバも、当業者ならわかるであろう。

【００１９】クライアント／サーバ構成では、たとえば装置１３によるサービスを必要とする装置１２（ｍ）は、必要なサービスを要求する１つまたは複数のメッセージ・パケットを生成して装置１３に送信する。この要求メッセージ・パケットには、装置１３、すなわち、メッセージ・パケットを受け取りサービスを実行する宛先装置のインターネット・アドレスが含まれる。装置１２（ｍ）は、要求メッセージ・パケットをＩＳＰ１１に送信する。ＩＳＰ１１は、そのメッセージ・パケットをインターネットを介して装置１３に転送する。装置１３がＷＡＮまたはＬＡＮの形態の場合、ＷＡＮまたはＬＡＮがメッセージ・パケットを受け取り、それをそのＷＡＮまたはＬＡＮに接続され、要求されたサービスを提供する特定の装置に宛てて送る。

【００２０】いずれの場合も、要求されたサービスを提供する装置１３は、要求メッセージ・パケットを受け取った後、その要求を処理する。要求メッセージ・パケットを生成した装置１２（ｍ）またはその操作者が、装置

１３に対して要求メッセージ・パケットを生成したそのサービスを要求するのに必要な許可を持っている場合、要求されたサービスが記憶サーバとしての装置１３からクライアントとしての装置１２（ｍ）への情報の伝送を開始することである場合は、装置１３は、要求された情報を含む１つまたは複数の応答メッセージ・パケットを生成し、そのパケットをインターネット１４を介してＩＳＰ１１に送る。次にＩＳＰ１１はそのメッセージ・パケットを装置１２（ｍ）に送る。一方、要求されたサービスが計算サーバとしての装置１３による処理を開始することである場合は、装置１３は要求された計算サービスを実行する。さらに、装置１３が計算中に生成された処理済みデータをクライアントとしての装置１２（ｍ）に返す必要がある場合、装置１３は、処理済みデータを含む１つまたは複数の応答メッセージ・パケットを生成し、そのパケットをインターネット１４を介してＩＳＰ１１に送る。次にＩＳＰ１１はそのメッセージ・パケットを装置１２（ｍ）に送る。サーバ装置１３が提供できる他のタイプのサービスに関しても、対応する操作を装置１２（ｍ）および１３、ＩＳＰ１１、およびインターネット１４によって実行することができる。

【００２１】上述のように、インターネット１４を介して送信するために装置１２（ｍ）および１３によって生成された各メッセージ・パケットには、スイッチング・ノードがそれぞれのメッセージ・パケットを適切な宛先装置に経路指定するために使用する宛先アドレスが含まれる。インターネットを介したアドレスは、「ｎ」ビット整数の形態をとる（ただし「ｎ」は現在、３２または１２８とすることができる）。特に、装置１２（ｍ）の操作者が、インターネットを介した送信のためのメッセージ・パケットの生成を開始するために、特定のインターネット・アドレスを覚えてそれらを装置１２（ｍ）に供給しなくても済むようにするために、インターネットはそれぞれの装置の操作者がより容易に使用できる第２のアドレス指定機構を備える。このアドレス指定機構では、ＬＡＮ、インターネット・サービス・プロバイダ（「ＩＳＰ」）など、インターネットに接続されたインターネット・ドメインは、人間にとって比較的読みやすい名前で識別される。人間可読ドメイン名に対応するために、ＩＳＰ１１は、ネームサーバ１７（ＤＮＳサーバとも呼ばれることがある）に関連づけられている。ネームサーバは、人間可読ドメイン名を変換して、それぞれの人間可読名で呼ばれている宛先の適切なインターネット・アドレスを提供することができる。一般に、ネームサーバはＩＳＰ１１の一部とするか、または図１に示すようにＩＳＰ１１に直接接続することができる。あるいは、インターネットでＩＳＰを介してアクセス可能な特定の装置とすることもできる。いずれの場合も、前述のように、通信セッション中に装置１２（ｍ）がＩＳＰ１１にログオンすると、ＩＳＰ１１は、装置１２（ｍ）が通信セッション中に使用する様々なインターネット・プロトコル（「ＩＰ」）パラメータを割り当てる。このパラメータはインターネット・パラメータ・ストア２５に記憶される。これらのＩＰパラメータには、（ａ）通信セッション中に装置１２（ｍ）を識別するインターネット・アドレスと、（ｂ）通信セッション中に装置１２（ｍ）が使用するネームサーバ１７の識別情報などの情報が含まれる。

【００２２】装置１２（ｍ）は、送信のためにメッセージ・パケットを生成するとき、その装置１２（ｍ）のインターネット・アドレス（上記の項目（ａ））を送信元アドレスとして含める。それぞれのメッセージ・パケットを受け取る装置１３は、装置１２（ｍ）から受け取ったメッセージ・パケットの中からこの送信元アドレスを使用することができ、それによって、それぞれの装置１３によって生成されたメッセージ・パケットを装置１２（ｍ）に経路指定することができる。装置１２（ｍ）がインターネット１４を介してネームサーバ１７にアクセスする場合、ＩＳＰ１１によって提供されるネームサーバ識別情報（上記の項目（ｂ））は、整数インターネット・アドレスの形態をとり、これによって、装置１２（ｍ）はネームサーバ１７に対して人間可読インターネット・アドレスから整数インターネット・アドレスへの変換を要求するメッセージを生成することができる。ＩＳＰ１１は、装置１２（ｍ）がＩＳＰ１１にログオンすると、装置１２（ｍ）に他のＩＰパラメータも割り当てることができる。これには、たとえば、特にＩＳＰが複数のゲートウェイを有する場合に装置１２（ｍ）によって送信されるメッセージに使用されるインターネット１４への接続の識別情報が含まれる。一般に、装置１２（ｍ）は、通信セッション中に使用するためにインターネット・パラメータをインターネット・パラメータ・ストア２５に記憶する。

【００２３】装置１２（ｍ）を操作する操作者が、装置１２（ｍ）から装置１３にメッセージ・パケットを送信することができるようにしたい場合、操作者はオペレータ・インタフェース２０を介して装置１３のインターネット・アドレスと、そのメッセージで送信する装置１２（ｍ）が維持する情報またはその識別情報を装置１２（ｍ）に供給する。オペレータ・インタフェース２０は、ＩＳＰ１１を介してインターネット１４で送信するために、その必要なパケットに対してパケット・ジェネレータ２２をイネーブルにする。パケット・ジェネレータ２２は、（ｉ）操作者が整数インターネット・アドレスを供給した場合、または（ii）操作者が人間可読インターネット・アドレスを供給したが、パケット・ジェネレータ２２が操作者によって供給された人間可読インターネット・アドレスに対応するすでに整数インターネット・アドレスを持っている場合、オペレータ・インタフェース２０によってイネーブルにされるとパケットを直

接生成し、それらをＩＳＰ１１に送信するためにネットワーク・インタフェース２１に供給することができる。

【００２４】しかし、操作者が、パケットの送信先である装置１３の人間可読インターネット・アドレスを供給した場合、および、パケット・ジェネレータ２２がまだそれに対応する整数インターネット・アドレスをもっていない場合、パケットジェネレータ２２は、ＩＰパラメータ・ストア２５で識別されているネームサーバ１７からネットワーク・アドレスを入手する。その操作に際して、パケット・ジェネレータ２２は、最初にネームサーバ１７に接触してネームサーバ１７から適切な整数インターネット・アドレスの入手を試みる。これらの操作で、装置１２（m）は、ネームサーバ１７に送信するための適切なメッセージ・パケットを、装置１２（m）が通信セッションの始めにログオンしたＩＳＰ１１によって提供されたネームサーバの整数インターネット・アドレスを使用して生成する。いずれの場合も、ネームサーバ１７が人間可読名の整数インターネット・アドレスを持っているかまたは入手可能な場合、ネームサーバ１７は装置１２（m）に整数インターネット・アドレスを供給する。この整数インターネット・アドレスを、パケット・ジェネレータ２２はネットワーク・インタフェース２１およびパケット受信および処理機能要素２３を介して受け取る。パケット・ジェネレータ２２は整数インターネット・アドレスを受け取った後、ネットワーク・インタフェース２１およびＩＳＰ１１を介して装置１３に送信するために、必要なメッセージ・パケットを生成する。

【００２５】前述のように、インターネット１４に接続された装置１３の１つは仮想私設ネットワーク１５であり、この仮想私設ネットワーク１５は、ファイアウォール３０と、サーバ３１（ｓ）として識別された複数の装置と、ネームサーバ３２とを含み、これらは通信リンク３３によって相互接続されている。サーバ３１（ｓ）、ファイアウォール３０、およびネームサーバ３２は、ＬＡＮまたはＷＡＮで接続された装置として、それらの装置の間でメッセージ・パケットの形態の情報を送信することができる。ファイアウォール３０はインターネット１４に接続され、インターネット１４を介してメッセージ・パケットを受信することができるため、インターネット・アドレスを有する。さらに、少なくとも、インターネットを介してアクセスすることができるサーバ３１（ｓ）も、それぞれのインターネット・アドレスを有し、その接続で、ネームサーバ３２は、仮想私設ネットワーク１５内部のサーバ３１（ｓ）のための人間可読インターネット・アドレスをそれぞれの整数インターネット・アドレスに変換する役割を果たす。

【００２６】一般に、仮想私設ネットワーク１５は、サーバ３１（ｓ）が仮想私設ネットワーク１５の外部の他の装置にアクセスしてその装置にインターネット１４を介して情報を送信することができるようにしたいが、装置１２（m）およびその他の装置によるサーバ３１（ｓ）へのインターネット１４を介したアクセスを制御された方式で制限したい会社、政府機関、組織などによって維持されている。ファイアウォール３０は、仮想私設ネットワーク１５内のサーバ３１（ｓ）への、仮想私設ネットワーク１５の外部の装置によるアクセスを制御する役割を果たす。その操作に際して、ファイアウォール３０は、インターネット１４にも接続し、インターネット１４から、サーバ３１（ｓ）に送るためのメッセージ・パケットを受け取る。メッセージ・パケットが、メッセージ・パケットの送信元が特定のサーバ３１（ｓ）へのアクセスを要求していることを示している場合、および送信元がサーバ３１（ｓ）へのアクセスを許可されている場合、ファイアウォール３０はメッセージ・パケットを通信リンク３３を介してサーバ３１（ｓ）に転送する。他方、送信元がサーバ３１（ｓ）へのアクセスを許可されていない場合、ファイアウォール３０はメッセージ・パケットをサーバ３１に転送せず、その代わりに、送信元がサーバ３１（ｓ）へのアクセスを許可されていなかったことを示す応答メッセージ・パケットを送信元装置に送る。ファイアウォールは、仮想私設ネットワーク１５内の他の装置３１（ｓ）と類似のものとすることができるが、参照番号４３で一般的に示す、インターネットへの１つまたは複数の接続が追加されている。

【００２７】装置１２（m）などの仮想私設ネットワーク１５の外部の装置と、仮想私設ネットワーク１５内部のサーバ３１（ｓ）などの装置との間の通信は、前述のようにファイアウォール３０と外部装置との間のセキュア・トンネルを介して維持することができ、それらの間で伝送される情報をインターネット１４でＩＳＰ１１を介して伝送されている間機密に維持することができる。装置１２（m）と仮想私設ネットワーク１５との間のセキュア・トンネルは、図１で参照番号４０、４２、および４４によって識別されている論理接続で表されている。論理接続４２は、ＩＳＰ１１とインターネット１４との間の論理接続４１のうちの１つを含み、論理接続４４はインターネット１４とファイアウォール３０の間の論理接続４３のうちの１つを含むことがわかるであろう。

【００２８】セキュア・トンネルの確立は、仮想ネットワーク１５の外部である装置１２（m）によって開始される。その操作に際して、装置１２（m）は操作者からの要求に応答して、装置１２（m）とファイアウォール３０との間のセキュア・トンネルの確立を要求するメッセージ・パケットを生成し、ＩＳＰ１１およびインターネット１４を介してファイアウォール３０に送信する。メッセージ・パケットは、ファイアウォール３０に関連づけられた所定の整数インターネット・アドレスに宛てて送られる。そのアドレスは、セキュア・トンネル確立

要求のために取ってあり、ネームサーバ１７にわかっており、ネームサーバ１７によって装置１２（m）に供給される。装置１２（m）が仮想私設ネットワーク１５内のサーバ３１（s）へのアクセスを許可されている場合、クライアント１２（m）とファイアウォール３０は、インターネット１４を介して両者の間で伝送される１つまたは複数のメッセージ・パケットを含む対話を行う。この対話中、ファイアウォール３０は装置１２（m）に、仮想私設ネットワークが装置１２（m）に送るメッセージ・パケットの暗号化された部分を装置１２（m）が復号する際に使用する復号アルゴリズムとそれに付随する復号鍵の識別情報を提供することができる。さらに、ファイアウォール３０は、装置１２（m）に、装置１２（m）が仮想私設ネットワーク１５に送信するメッセージ・パケットの暗号化される部分を暗号化する際に装置１２（m）が使用する、暗号化アルゴリズムとそれに付随する暗号鍵の識別情報も提供することができる。あるいは、装置１２（m）がこの暗号化アルゴリズムと鍵の識別情報を提供することができ、それをファイアウォール３０が対話中に使用する。装置１２（m）は、ファイアウォール３０の識別情報と、セキュア・トンネルを介して伝送されるメッセージ・パケットの暗号化アルゴリズムおよび復号アルゴリズムおよびそれらに付随する鍵の識別情報を関連づける情報を含む、セキュア・トンネルに関する装置１２（m）のＩＰパラメータ２５情報を記憶することができる。

【００２９】その後、装置１２（m）とファイアウォール３０は、このセキュア・トンネルを介してメッセージ・パケットを送信することができる。装置１２（m）は、セキュア・トンネルを介した転送のためにメッセージ・パケットを生成する際に、インターネット１４を介してファイアウォール３０に送信するためにネットワーク・インタフェース２１によってＩＳＰ１１に送信する前に、メッセージ・パケットのうちの暗号化すべき部分を暗号化するためと、装置１２（m）が受け取ったメッセージ・パケットの暗号化された部分を復号するために、セキュア・パケット処理機能要素２６を使用する。具体的には、パケット・ジェネレータ２２は、セキュア・トンネルを介してファイアウォール３０に送信するためにメッセージ・パケットを生成した後、そのメッセージ・パケットをセキュア・パケット処理機能要素２６に供給する。セキュア・パケット処理機能要素２６は、暗号化アルゴリズムおよび鍵を使用して、メッセージ・パケットの暗号化すべき部分を暗号化する。ファイアウォール３０は、セキュア・トンネルを介して装置１２（m）からメッセージ・パケットを受け取った後、それを復号し、メッセージ・パケットの意図された受信者が仮想私設ネットワーク１５内のサーバ３１（s）などの別の装置である場合、ファイアウォール３０はメッセージ・パケットを通信リンク３３を介してその別の装置に送る。

【００３０】セキュア・トンネルを介して仮想私設ネットワーク１５内のサーバ３１（s）などの装置によって装置１２（m）に送信されるメッセージ・パケットの場合、ファイアウォール３０はそのようなメッセージ・パケットを通信リンク３３を介して受け取り、そのメッセージ・パケットを暗号化し、インターネット１４を介してＩＳＰ１１に送る。ＩＳＰ１１はそのメッセージ・パケットを装置１２（m）、詳細にはネットワーク・インタフェース２１に転送する。ネットワーク・インタフェース２１は、メッセージ・パケットをセキュア・パケット処理機能要素２６に供給し、セキュア・パケット処理機能要素２６は復号アルゴリズムおよび鍵を使用してメッセージ・パケットの暗号化部分を復号する。

【００３１】仮想私設ネットワーク１５の外部にある装置１２（m）などの装置と、ファイアウォールの外部にあるサーバ３１（s）などの装置によるアクセスに関して問題が生じる。すなわち、ネームサーバ１７に、ファイアウォール３０に関連づけられた整数インターネット・アドレス以外の、仮想私設ネットワーク１５内にあるサーバ３１（s）およびその他の装置の整数インターネット・アドレスが提供されなていないことである。したがって、装置１２（m）は、操作者が人間可読インターネット・アドレスを入力した後で、そのネームサーバ１７からアクセスされるサーバ３１（s）の整数インターネット・アドレスを入手することができない。

【００３２】この問題に対処するために、装置１２（m）とファイアウォール３０が協調して両者の間にセキュア・トンネルを確立するときに、セキュア・トンネルを介して送信されるメッセージ・パケットと共に使用される暗号化および復号のアルゴリズムおよび鍵の識別情報を装置１２（m）に提供することができる他に、ファイアウォール３０は装置１２（m）に対して、装置１２（m）の操作者が供給することができる人間可読インターネット・アドレスの適切な整数インターネット・アドレスを装置１２（m）が入手するためにアクセスできる、仮想私設ネットワーク１５内のネームサーバ３２などのネームサーバの識別情報も提供する。ネームサーバ３２の識別情報も、通信セッションの始めに装置１２（m）がＩＳＰ１１にログオンしたときにＩＳＰ１１によって提供されたネームサーバ１７の識別情報と共にＩＰパラメータ・ストア２５に記憶される。したがって、装置１２（m）が、たとえば操作者によって供給された人間可読インターネット・アドレスを使用して、仮想私設ネットワーク１５内のサーバ３１（s）などの装置にメッセージ・パケットを送信する場合、装置１２（m）は前述のように最初にネームサーバ１７にアクセスして、人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスの入手を試行する。ネームサーバ１７は仮想私設ネットワーク１５の外部にあ

り、装置１２（m）によって要求された情報を持たないため、それを示す応答メッセージ・パケットを送信する。装置１２（m）はその後で、要求メッセージ・パケットを生成し、ファイアウォール３０とセキュア・トンネルを介してネームサーバ３２に送信する。ネームサーバ３２が装置１２（m）によって供給された要求メッセージ・パケット内の人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを持っている場合、ネームサーバ３２はネームサーバ１７に関連して前述したのとほぼ同様の方式で整数インターネット・アドレスを提供する。ただし、ネームサーバ３２は、この整数インターネット・アドレスをファイアウォール３０に宛てられたメッセージ・パケットで供給し、ファイアウォール３０はその後でそのメッセージ・パケットをセキュア・トンネルを介して装置１２（m）に送信する。ファイアウォール３０によって送信されるメッセージ・パケットでは、メッセージ・パケット内の整数インターネット・アドレスはセキュア・トンネルを介して伝送されるメッセージ・パケットのデータ部分に入れられ、したがって、暗号化形式をとる。メッセージ・パケットは、装置１２（m）がセキュア・トンネルを介して受け取る他のメッセージ・パケットに関して前述したのと同様の方式で装置１２（m）によって処理される。すなわち、メッセージ・パケットは、処理のためにパケット受信および処理機能要素２３に供給される前に、セキュア・パケット処理機能要素２６によって復号される。サーバ３１（s）の整数インターネット・アドレスは、それに対する人間可読インターネット・アドレスとの関連づけと、その人間可読インターネット・アドレスに関連づけられたサーバ３１（s）に仮想私設ネットワーク１５のファイアウォールを介してアクセスする必要があることを示す標識と、サーバ３１（s）に対して送信され、サーバ３１（s）が受け取るメッセージ・パケットの適切な部分の暗号化および復号に使用される暗号化および復号のアルゴリズムおよび鍵の識別情報と共に、ＩＰパラメータ・ストア２５内のアクセス制御リスト（「ＡＣＬ」）にキャッシュすることができる。

【００３３】装置１２（m）によって供給された人間可読インターネット・アドレスの整数インターネット・アドレスをネームサーバ３２に要求する装置１２（m）からのメッセージ・パケットにネームサーバが応答する際、ネームサーバ３２がその人間可読インターネット・アドレスと整数インターネット・アドレスとの間の関連づけを持っていない場合、ネームサーバ３２はそれを示す応答メッセージ・パケットを送ることができる。装置１２（m）が、装置１２（m）がアクセスすることができる他の仮想私設ネットワーク（図示せず）に関連づけられている可能性のあるネームサーバなど、他のネームサーバの識別情報を持っている場合、装置１２（m）は上述と同様の方式で他のネームサーバにアクセスを試みることができる。装置１２（m）が、アクセスすることができ、装置１２（m）のＩＰパラメータ・ストア２５内で一般的に識別されるいずれのネームサーバからもその人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを入手することができない場合、装置１２（m）は、人間可読インターネット・アドレスを持っている装置にアクセスことができず、アクセスを要求した操作者またはプログラムにそれを通知する。

【００３４】これを背景にして、本発明と共に装置１２（m）および仮想私設ネットワーク１５によって実行される操作について以下に詳述する。一般に、操作は２段階で進む。第１段階では、装置１２（m）と仮想私設ネットワーク１５が協調して、インターネット１４を介したセキュア・トンネルを確立する。この第１段階で、仮想私設ネットワーク１５、詳細にはファイアウォール３０が、ネームサーバ３２の識別情報を提供し、前述のように暗号化および復号のアルゴリズムおよび鍵情報も提供することができる。第２段階では、セキュア・トンネルが確立された後、装置１２（m）は、第１段階中にファイアウォール３０によって識別されたネームサーバ３２から、必要に応じて人間可読インターネット・アドレスから整数インターネット・アドレスへの変換を入手するプロセスで、仮想私設ネットワーク１５内の１つまたは複数のサーバ３１（s）へのメッセージ・パケットの生成と送信に関して第１段階で提供された情報を使用することができる。

【００３５】したがって、第１の（セキュア・トンネル確立）段階では、装置１２（m）は最初に、ファイアウォール３０への送信のためにセキュア・トンネルの確立を要求するメッセージ・パケットを生成する。このメッセージ・パケットには、ファイアウォールの整数インターネット・アドレス（装置の操作者または装置１２（m）によって処理されているプログラムによって供給されたか、または操作者またはプログラムによって人間可読インターネット・アドレスが供給された後でネームサーバ１７によって供給されたもの）、詳細には、ファイアウォール３０がそれとのセキュア・トンネルを確立することができるようにするためのアドレスが含まれる。ファイアウォール３０がセキュア・トンネル確立要求を受け入れる場合、およびファイアウォール３０が前述のように暗号化および復号アルゴリズムおよび鍵を提供する場合、ファイアウォールは、その暗号化および復号アルゴリズムおよび鍵を識別する応答メッセージ・パケットを、装置１２（m）への送信のために生成する。装置１２（m）が応答メッセージを受け取ると、暗号および復号アルゴリズムおよび復号アルゴリズムおよび鍵の識別情報はＩＰパラメータ・ストア２５に記憶される。

【００３６】第１段階のうちの後の時点で、ファイアウ

ォール３０は、装置１２（m）に送信するためにネームサーバ３２の整数インターネット・アドレスを含むメッセージ・パケットも生成する。このメッセージ・パケットの場合、メッセージ・パケットのうちのネームサーバ３２の整数インターネット・アドレスを含む部分が、暗号化アルゴリズムおよび鍵を使用して暗号化され、それを、前述の応答メッセージ・パケットで提供される復号アルゴリズムおよび鍵を使用して復号することができる。このメッセージは一般に以下のような構造を有する。

”＜ＩＩＡ（FW），ＩＩＡ（DEV１２（m））＞SEC_TUN＞＜ENCR＜＜ＩＩＡ（FW），ＩＩＡ（DEV_１２（m））＞＜DNS_ADRS：ＩＩＡ（NS_３２）＞＞＞”上記で、（ｉ）”ＩＩＡ（FW）”は送信元アドレス、すなわちファイアウォール３０の整数インターネット・アドレスを表し、（ii）”ＩＩＡ（DEV_１２（m））”は宛先アドレス、すなわち装置１２（m）の整数インターネット・アドレスを表し、（iii）”DNS_ADRS：ＩＩＡ（NS）は、”ＩＩＡ（NS_３２）”が装置１２（m）が使用を許可されているネームサーバ３２の整数インターネット・アドレスを表すことを示し、（iv）”ENCR＜．．．＞”は、大括弧”＜”と”＞”の間の情報が暗号化されることを示す。メッセージの最初の部分最初の部分”＜ＩＩＡ（FW），ＩＩＡ（DEV_１２（m））”は、メッセージのヘッダ部の少なくとも一部を形成し、”＜ENCR＜＜ＩＩＡ（FW），ＩＩＡ（DEV_１２（m））＞＜ＩＩＡ（NS）＞＞＞”は、メッセージのデータ部の少なくとも一部を表す。”＜SEC_TUN＞”は、ヘッダ内のセキュア・トンネルを介して伝送されるメッセージを示す標識を表し、それによってメッセージのデータ部に暗号化情報が含まれていることを示す。

【００３７】装置１２（m）が前述のようにファイアウォール３０からメッセージを受け取った後、メッセージ・パケットには＜SEC_TUN＞標識が含まれているため、装置１２（m）のネットワーク・インタフェース２１は暗号化部分”＜ENCR＜＜ＩＩＡ（FW），ＩＩＡ（DEV_１２（m））＞＜DNS_ADRS：ＩＩＡ（NS_３２）＞＞＞”を、処理のためにセキュア・パケット処理機能要素２６に送る。セキュア・パケット処理機能要素は、暗号化部分を復号し、”ＩＩＡ（NS_３２）”部分がネームサーバ、装置１２（m）が使用することを許可されている特にネームサーバ３２の整数インターネット・アドレスであると判断し、そのアドレスを、それに送られるメッセージ・パケットがファイアウォール３０に転送すべきであることと、ファイアウォール３０によって前もって提供された暗号化アルゴリズムおよび鍵を使用してメッセージ・パケット内のデータを暗号化すべきであることを示す標識と共に、ＩＰパラメータ・ストア２５に記憶する。ネームサーバ３２の整数インターネット・アドレスはファイアウォールから装置１２（m）に暗号化形式で送られるため、パケットが第三者によって傍受された場合でも機密に維持される。

【００３８】セキュア・トンネルの確立に使用される特定のプロトコルによっては、ファイアウォール３０と装置１２（m）は上述の情報以外の情報を含むメッセージ・パケットを交換することもできる。

【００３９】前述のように、第２段階では、セキュア・トンネルが確立された後、装置１２（m）は第１段階中に提供された情報を、メッセージ・パケットの生成と、仮想私設ネットワーク１５内のサーバ３１（ｓ）のうちの１つまたは複数のサーバへの送信に関して使用することができる。これらの操作に際して、装置１２（m）の操作者または装置１２（m）によって処理されているプログラムが、装置１２（m）に仮想私設ネットワーク１５内のサーバ３１（ｓ）に対してメッセージ・パケットを送信させたい場合、オペレータ・インタフェース２０を介して操作者が、またはプログラムが人間可読インターネット・アドレスを供給した場合、装置１２（m）、詳細にはパケット・ジェネレータ２２は、最初にＩＰパラメータ・ストア２５がその中にその人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスをキャッシュしているかどうかを判断する。キャッシュしていない場合、パケット・ジェネレータ２２は、人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを供給するように要求する要求メッセージ・パケットを生成し、ネームサーバ１７に送る。ネームサーバがその人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを持っている場合、ネームサーバ１７はその整数インターネット・アドレスを装置１２（m）に供給する。これは、要求メッセージ・パケット内の人間可読インターネット・アドレスが仮想私設ネットワーク１５の外部の装置１３に関連づけられていた場合にも、仮想私設ネットワーク１５内のサーバ３２（ｓ）に関連づけられていた場合にも行われれることがわかるであろう。その後、装置１２（m）は、前述のように、インターネットを介して送信するためにその整数インターネット・アドレスを使用してメッセージ・パケットを生成することができる。

【００４０】一方、ネームサーバ１７がその人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを持っていない場合、ネームサーバ１７は装置１２（m）にそれを示す応答メッセージ・パケットを送る。その後、装置１２（m）のパケット・ジェネレータ２２が、そのＩＰパラメータ・ストア２５で識別されている次のネームサーバに送信するための要求メッセージ・パケットを生成し、そのネームサーバに対し

てその人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを提供するように要求する。この、次のネームサーバがネームサーバ３２である場合、パケット・ジェネレータ２２はメッセージ・パケットを処理のためにセキュア・パケット処理機能要素２６に送る。セキュア・パケット処理機能要素２６は、セキュア・トンネルを介してファイアウォール３０に送る要求メッセージ・パケットを生成する。このメッセージは一般に以下のような構造を有する。

”＜ＩＩＡ（ＤＥＶ＿１２（ｍ）），ＩＩＡ（ＦＷ）＞＜ＳＥＣ＿ＴＵＮ＞＜ＥＮＣＲ＜＜ＩＩＡ（ＤＥＶ＿１２（ｍ）），ＩＩＡ（ＮＳ＿３２））＞＜ＩＩＡ＿ＲＥＱ＞＞＞”上記で、（ｉ）”＜ＩＩＡ（ＤＥＶ＿１２（ｍ））”は送信元アドレス、すなわち装置１２（ｍ）の整数インターネット・アドレスを表し、（ｉｉ）”ＩＩＡ（ＦＷ）”は宛先アドレス、すなわちファイアウォール３０の整数インターネット・アドレスを表し、（ｉｉｉ）”ＩＩＡ（ＮＳ＿３２）”はネームサーバ３２のアドレスを表し、（ｉｖ）”＜ＩＩＡ（ＤＥＶ＿１２（ｍ）），ＩＩＡ（ＮＳ＿３２））＞＜ＩＩＡ＿ＲＥＱ＞＞”は、パケット・ジェネレータ２２によって生成された要求メッセージ・パケットを表し、”＜ＩＩＡ（ＤＥＶ＿１２（ｍ）），ＩＩＡ（ＮＳ＿３２＞”は要求メッセージ・パケットのヘッダ部を表し、”＜ＩＩＡ＿ＲＥＱ＞”は要求メッセージ・パケットのデータ部を表し、（ｖ）”ＥＮＣＲ＜．．．＞”は、大括弧”＜”と”＞”の間の情報が暗号化されていることを表し、（ｖｉ）”＜ＳＥＣ＿ＴＵＮ＞”は、セキュア・パケット・ジェネレータ２２によって生成されたメッセージ・パケットのヘッダ部内にある標識であって、メッセージがセキュア・トンネルを介して送信されることを示し、それによって、メッセージのデータ部に暗号化情報が含まれていることを示す。

【００４１】ファイアウォール３０は、セキュア・パケット処理機能要素２６によって生成された要求メッセージ・パケットを受け取ると、メッセージ・パケットの暗号化部分を復号して、要求メッセージ・パケットがパケット・ジェネレータ２２によって生成されたことを表す＜＜ＩＩＡ（ＤＥＶ＿１２（ｍ）），ＩＩＡ（ＮＳ＿３２））＞＜ＩＩＡ＿ＲＥＱ＞＞”を入手する。要求メッセージ・パケットを入手した後、ファイアウォール３０はそれを通信リンク３３を介してネームサーバ３２に送る。このプロセスの際、通信リンク３３を介してメッセージ・パケットを送信するプロトコルによっては、ファイアウォール３０は通信リンク３３のプロトコルに準拠するように要求パケットを修正する必要がある場合もある。

【００４２】ネームサーバ３２は、要求メッセージ・パケットを受け取った後、それを処理して、ネームサーバ３２が要求メッセージ・パケットで供給された人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを持っているかどうかを判断する。ネームサーバがそのような整数インターネット・アドレスを持っていると判断した場合、ネームサーバはファイアウォールに送信するためにその整数インターネット・アドレスを含む応答メッセージ・パケットを生成する。一般に、この応答メッセージ・パケットは以下の構造を有する。

＜＜ＩＩＡ（ＮＳ＿３２），ＩＩＡ（ＤＥＶ＿１２（ｍ））＞＜ＩＩＡ＿ＲＥＳＰ＞＞上記で、（ｉ）”ＩＩＡ（ＮＳ＿３２）”は送信元アドレス、すなわちネームサーバ３２の整数インターネット・アドレスを表し、（ｉｉ）”ＩＩＡ（ＤＥＶ＿１２（ｍ））”は宛先アドレス、すなわち装置（１２（ｍ）の整数インターネット・アドレスを表し、（ｉｉｉ）”ＩＩＡ＿ＲＥＳＰ”は、人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを表す。

【００４３】ファイアウォール３０が応答メッセージ・パケットを受け取った後、装置１２（ｍ）との通信が両者の間のセキュア・トンネルを介するため、ファイアウォール３０はネームサーバ３２から受け取った応答メッセージ・パケットを暗号化し、装置１２（ｍ）に送信するためにその暗号化応答メッセージ・パケットを含むメッセージ・パケットを生成する。一般に、ファイアウォール３０によって生成されるメッセージ・パケットは以下の構造を有する。”＜ＩＩＡ（ＦＷ），ＩＩＡ（ＤＥＶ１２（ｍ））＞＜ＳＥＣ＿ＴＵＮ＞＜ＥＮＣＲ＜＜ＩＩＡ（ＮＳ＿３２），ＩＩＡ（ＤＥＶ＿１２（ｍ））＞＜ＩＩＡ＿ＲＥＳＰ＞＞＞”上記で、（ｉ）”ＩＩＡ（ＦＷ）”は送信元アドレス、すなわちファイアウォール３０の整数インターネット・アドレスを表し、（ｉｉ）”ＩＩＡ（ＤＥＶ＿１２（ｍ））”は宛先アドレス、すなわち装置１２（ｍ）の整数インターネット・アドレスを表し、（ｉｉｉ）”ＳＥＣ＿ＴＵＮ”は、セキュア・パケット・ジェネレータ２２によって生成されたメッセージ・パケットのヘッダ部内の、メッセージがセキュア・トンネルを介して送信されることを示す標識を表し、それによってメッセージのデータ部に暗号化情報が含まれていることを示し、（ｉｖ）”ＥＮＣＲ＜．．．＞”は、”＜”と”＞”の間の情報（ネームサーバ３２から受け取った応答メッセージ・パケットを構成する）が暗号化されていることを示す。

【００４４】さらに、通信リンク３３を介したメッセージ・パケットの送信のためのプロトコルによっては、ファイアウォール３０はインターネット１４のプロトコルに準拠するようにメッセージ・パケットを処理および／または修正する必要がある場合がある。

【００４５】装置１２（ｍ）がファイアウォール３０からメッセージ・パケットを受け取ると、そのメッセージ・パケットはセキュア・パケット処理機能要素２６に送

られる。セキュア・パケット処理機能要素２６は、メッセージ・パケットの暗号化部分を復号し、人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを入手し、その情報をＩＰパラメータ・ストア２５にロードする。その後、装置はその整数インターネット・アドレスを、人間可読インターネット・アドレスに関連づけられたサーバ３１（ｓ）に送信するためのメッセージ・パケットの生成に使用することができる。

【００４６】要求メッセージ・パケットで装置１２（ｍ）から送られた人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスをネームサーバ３２が持っていなかった場合、ネームサーバ３２はネームサーバ３２によって生成される応答メッセージ・パケットでそれを示すことができることがわかるであろう。ファイアウォール３０は、ネームサーバ３２から送られた応答メッセージに応答し、装置１２（ｍ）に送信するために、ネームサーバ３２によって生成された応答メッセージ・パケットを含む暗号化部分が入ったメッセージ・パケットも生成する。装置１２（ｍ）がメッセージ・パケットを受け取った後、暗号化部分はセキュア・パケット処理機能要素２６によって復号され、セキュア・パケット処理機能要素２６はパケット・ジェネレータ２２に、その人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスをネームサーバ３２が持っていないことを通知する。その後、ＩＰパラメータ・ストア２５に別のネームサーバの識別情報が入っている場合、装置１２（ｍ）のパケット・ジェネレータ２２はそのＩＰパラメータ・ストア２５で識別されている次のネームサーバに送信するために要求メッセージ・パケットを生成し、そのネームサーバに人間可読インターネット・アドレスに関連づけられた整数インターネット・アドレスを供給するように要求する。それに対して、ＩＰパラメータ・ストア２５に別のネームサーバの識別情報が入っていない場合、パケット・ジェネレータ２２は、オペレータ・インタフェース２０またはプログラムに対して、それによって供給された人間可読インターネット・アドレスに関連づけられた装置に送信するためのメッセージ・パケットを生成することができないことを通知する。

【００４７】本発明にはいくつかの利点がある。具体的には、本発明は、セキュア・トンネルを介して私設ネットワークに接続されたネームサーバによる人間可読アドレスからネットワーク・アドレスへの変換を容易にすることによって、インターネット１４などの公衆ネットワークに接続された装置と、仮想私設ネットワーク１５などの私設ネットワークに接続された装置と間の通信を容易にするシステムを提供する。

【００４８】図１に関して前述した構成には多くの変更を加えることができることがわかるであろう。たとえば、ネットワーク１０について、暗号化および復号のアルゴリズムおよび鍵が、セキュア・トンネルが確立される対話中に装置１２（ｍ）とファイアウォールとの間で交換されるものとして説明したが、この情報は装置１２（ｍ）とファイアウォール３０によって両者の間のセキュア・トンネルの確立とは別に提供することもできることがわかるであろう。

【００４９】さらに、本発明についてインターネットに関して説明したが、本発明はどのようなネットワークと共にでも利用可能であることがわかるであろう。さらに、本発明について、人間可読ネットワーク・アドレスを備えるネットワークに関して説明したが、本発明はどのような形態の二次または非公式ネットワーク・アドレス構成を備えるどのようなネットワークと共にでも利用可能であることがわかるであろう。

【００５０】本発明によるシステムは全部または一部を、特殊目的ハードウェアまたは汎用コンピュータ・システム、あるいはその任意の組合せで構成することができ、そのどの部分も適合するプログラムによって制御可能であることがわかるであろう。どのプログラムもその全部または一部が、従来の方式でシステムの一部を含むかまたはシステム上に記憶することができる。あるいは、プログラムの全部または一部を従来の方式で情報を伝送するネットワークまたはその他の機構を介してシステム内に供給することができる。さらに、このシステムは、システムに直接接続可能な、または従来の方式で情報を伝送するネットワークまたはその他の機構を介してシステムに情報を伝送することができる操作者入力要素（図示せず）を使用して、操作者によって供給される情報を使用して操作および／または制御することができることがわかるであろう。

【００５１】以上の説明は、本発明の特定の実施形態に限られていた。しかし、本発明には様々な変形または修正を加えることができ、その際、本発明の利点の一部または全部が実現されることがわかるであろう。特許請求の範囲の目的は、上記およびその他の変形および修正を、本発明の精神および範囲に含まれるものとしてカバーすることである。

【図面の簡単な説明】

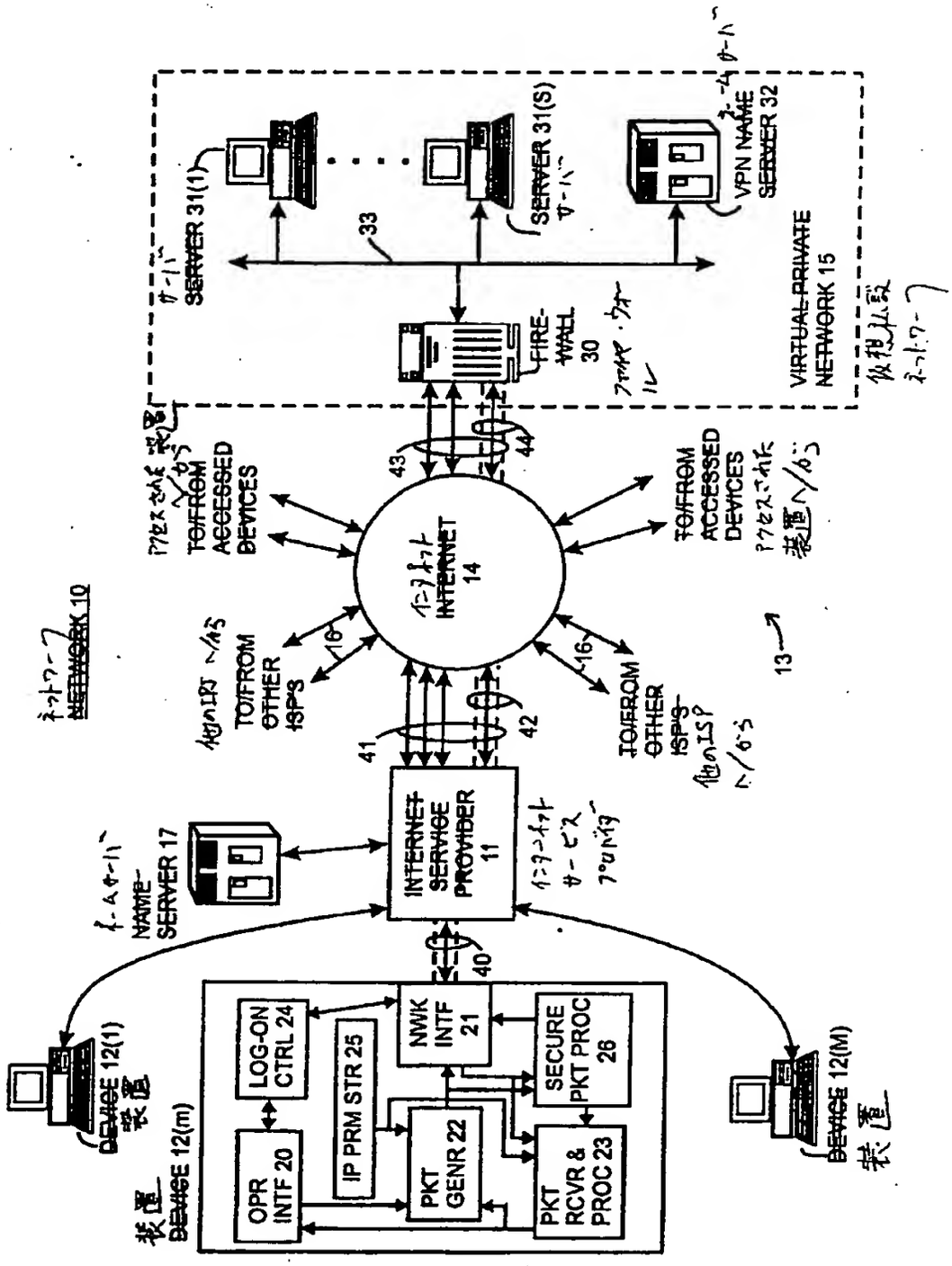
【図１】　本発明により構成されたネットワークを示す機能ブロック図である。

【符号の説明】

１０　ネットワーク
１２、１３　装置
１５　仮想私設ネットワーク
１７　ネームサーバ
２０　オペレータ・インタフェース
２１　ネットワーク・インタフェース
２２　パケット・ジェネレータ
２３　パケット受信および処理機能要素

２４　ログオン・コントロール
２５　インターネット・パラメータ・ストア
２６　セキュア・パケット処理機能要素
３０　ファイアウォール
３１　サーバ
３２　ネームサーバ

【図１】



フロントページの続き

(71)出願人　591064003
901 SAN ANTONIO ROAD
PALO ALTO, CA 94303, U.
S. A.

(72)発明者　ジョセフ・イー・プロビーノ
アメリカ合衆国・02138・マサチューセッツ州・ケンブリッジ・ウェンデル　ストリート・29